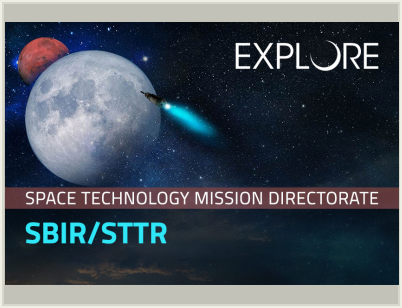
# Continuous Integrated Invariant Inference, Phase I

Completed Technology Project (2011 - 2011)

## Project Introduction

The proposed project will develop a new technique for invariant inference and embed this and other current invariant inference and checking techniques in an easy-to-use tool. The result will enhance an engineer's ability to use formal methods ⬌ generating, editing, reviewing, proving and testing invariants ⬌ and improve productivity in verification and validation of safety and correctness properties software. Currently, invariants that represent such properties require extensive human effort to write; automated techniques, though improving, are still insufficiently capable of automatically inferring them. The proposed project will develop innovative techniques to infer logical invariants describing the behavior of individual software modules by combining static (analyzing a program without running it) and hybrid analysis (inferring invariants from observations of executing software). In particular, the project will (a) combine concolic execution and hybrid analysis to find candidate invariants from high-branch-coverage test suites, (b) apply that combination to obtain invariants for individual functions and data structures, (c) iterate the analysis to broaden data coverage of the test suite and improve the accuracy of invariants, and (d) create early prototypes and development plans to integrate the resulting tools in selected IDEs (Eclipse and GrammaTech's CodeSonar tool). In carrying out this project, GrammaTech will build on its static analysis tools, concolic engine, and software dynamic translation module. It will leverage its base of research and expertise in static and hybrid analysis, specification languages, automated SMT theorem provers, and GUI tools for program analysis and development. The commercialization prospects for the proposed project are enhanced by GrammaTech's demonstrated experience in producing prototypes and commercial products from research results.



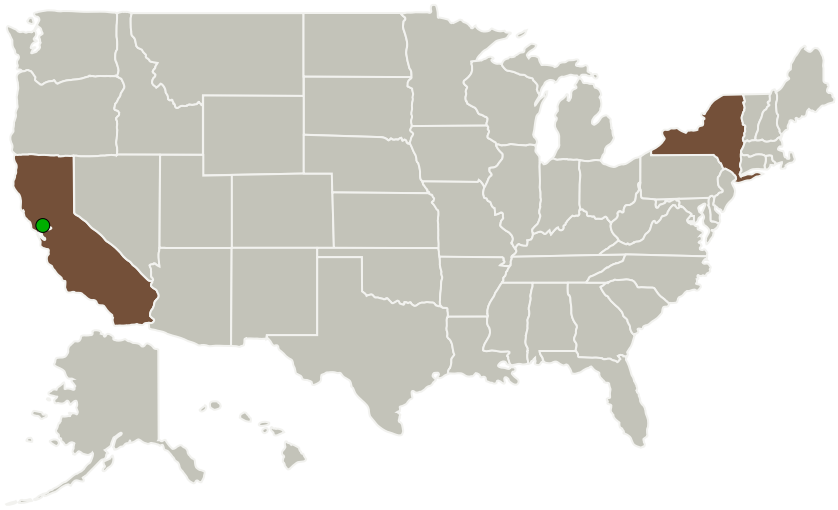

Continuous Integrated Invariant Inference, Phase I

## Table of Contents

# Continuous Integrated Invariant Inference, Phase I

Completed Technology Project (2011 - 2011)

## Primary U.S. Work Locations and Key Partners



| Organizations Performing Work | Role | Type | Location |
|---|---|---|---|
| GrammaTech, Inc. | Lead Organization | Industry | Ithaca, New York |
| Ames Research Center(ARC) | Supporting Organization | NASA Center | Moffett Field, California |

| Primary U.S. Work Locations | |
|---|---|
| California | New York |

## Project Transitions

**February 2011:** Project Start

**September 2011:** Closed out

**Closeout Documentation:**

- Final Summary Chart*(https://techport.nasa.gov/file/138060)*

## Organizational Responsibility

**Responsible Mission Directorate:**

Space Technology Mission Directorate (STMD)

**Lead Organization:**

GrammaTech, Inc.

**Responsible Program:**

Small Business Innovation Research/Small Business Tech Transfer

## Project Management

**Program Director:**

Jason L Kessler

**Program Manager:**

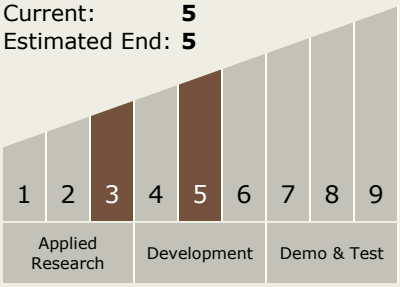
Carlos Torrez

**Principal Investigator:**

David Cok

## Technology Maturity (TRL)

Start: **3**
Current: **5**
Estimated End: **5**



# Continuous Integrated Invariant Inference, Phase I

Completed Technology Project (2011 - 2011)

## Technology Areas

**Primary:**

- TX04 Robotic Systems
  - TX04.6 Robotics Integration
    - TX04.6.3 Robot Software

## Target Destinations

The Sun, Earth, The Moon, Mars, Others Inside the Solar System, Outside the Solar System